EC-Council

C|PENT

Certified Penetration Testing Professional

Certified Penetration Testing Professional

Courseware

EC-COUNCIL OFFICIAL CURRICULUM

Certified Penetration Testing Professional

Version 1

EC-Council

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

NOTICE TO THE READER

Foreword

The dearth of quality penetration tester to thwart the security threats in a timely fashion is one of the major challenges organizations face today. Organizations need to hire experts in the field of computer security infrastructure or train in-house security administrators to fight IT security dangers if they are to stand any chance against attackers.

The increasingly networked corporate environment means that companies often having their websites as a single point of contact across geographical boundaries. This makes it critical to take countermeasures to prevent any exploits that can result in loss of important data.

A penetration test is an exercise that is used to assess the security of an organizational computer system or network. The exercise involves a series of tests simulating the possible attacks on the network from an attacker. A penetration test helps point out the vulnerabilities that can be exploited by an attacker and reveals the potential consequences of a real attacker breaking into the network. This information is then used to harden the network and can be an important tool for network administrators, IT managers, and executives. From a business perspective, a penetration test helps an organization prevent any financial loss through fraud attempts by external (hackers) or internal sources (disgruntled employees), helps protect the brand name from being tarnished due to a cyber-attack on the organization, and helps build the right strategies for protecting the information assets of the organization. Also, a penetration test helps in complying with various regulations and laws that govern information security.

The Certified Penetration Testing Professional (CPENT) program aims to armor the security professional with penetration testing techniques and tools to help them perform penetration tests and protect the information assets of their organization.

Program Introduction

Certified Penetration Testing Professional (CPENT) program is a comprehensive, standards-based, methodological approach to training and validating IT security professionals' Penetration Testing and IS Security Auditing capabilities. The program consists of a highly interactive 5-day security training class.

The CPENT training program is designed to teach security professionals the advanced uses of the available methodologies, tools, and techniques required to perform comprehensive information security tests. Security professionals will learn how to design, secure, and test networks to protect their organizations from the threats hackers and crackers pose. By teaching the LPT methodology and ground breaking techniques, this class helps security professionals perform the intensive assessments required to effectively identify and mitigate risks to the security of their infrastructure. As students learn to identify the security problems they also learn how to avoid and eliminate them, as the class provides complete coverage of analysis and network security-testing topics.

Certified Penetration Testing Professional (CPENT) complements the Certified Ethical Hacker (CEH) certification by exploring the analytical phase of ethical hacking. While CEH exposes the learner to attack vectors, hacking tools and technologies, CPENT takes it a step further by exploring how to analyze the outcome from these tools and technologies. Through ground-breaking penetration testing methodology and framework, the CPENT class helps students perform the intensive assessments required to effectively identify and mitigate risks to the security of information system infrastructures. The objective of CPENT training program is to increase the knowledge of experienced security professionals by helping them analyze the outcomes of their tests. CPENT leads the learner into the advanced stages of ethical hacking.

EC-Council's Certified Penetration Testing Professional (CPENT) program teaches you how to perform an effective penetration test in an enterprise network environment that must be attacked, exploited, evaded, and defended. If you have only been working in flat networks, CPENT's live practice range will teach you to take your skills to the next level by teaching you how to pen test IT systems, IoT systems, OT systems, how to write your own exploits, build your own tools, conduct advanced binaries exploitation, double pivot to access hidden networks, and also customize scripts/exploits to get into the innermost segments of the network.

The program also introduces the learners to the business aspect of penetration testing and makes CPENT a relevant milestone towards achieving EC-Council's Licensed Penetration Tester (LPT) Master certificate. The LPT Master certificate standardizes the knowledge base for penetration testing professionals by validating their skills and knowledge of best practices followed by the experienced experts in the field.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User

C|SCU
Certified | Secure Computer User

The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender

C|ND
Certified | Network Defender

Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Ethical Hacking: Certified Ethical Hacker

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Incident Handling: EC-Council Certified Incident Handler

EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally.It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

CPENT Exam Information

CPENT Exam Details	
Exam Title	**Certified Penetration Testing Professional (CPENT)**
Exam Code	**412-80**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**)
Duration	**24 Hours**
Passing Score	**70% (CPENT)** **90% (LPT Master)**

Please visit **https://www.eccouncil.org/programs/certified-penetration-testing-professional-cpent/** for more information.

Table of Contents